Dr.WEB®

Anti-virus for Mac OS X

Defend what you create

User Manual

Dr.Web Anti-virus for Mac OS X
Version 10.0.2
User Manual
29.10.2014

Doctor Web Head Office
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125124

Web site: www.drweb.com
Phone: +7 (495) 789-45-87

Refer to the official web site for regional and international office information.

Doctor Web

Doctor Web develops and distributes Dr.Web® information security solutions which provide efficient protection from malicious software and spam.

Doctor Web customers can be found among home users from all over the world and in government enterprises, small companies and nationwide corporations.

Dr.Web antivirus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards. State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

We thank all our customers for their support and devotion to the Dr.Web products!

Table of Contents

Document Conventions

The following conventions and symbols are used in this manual:

Convention	Description
Bold	Names of buttons and other elements of the graphical user interface (GUI), and required user input that must be entered exactly as given in the guide.
Green and bold	Names of **Dr.Web** products and components.
Green and underlined	Hyperlinks to topics and web pages.
Italic	Placeholders which represent information that must be supplied by the user. For command-line input, it indicates parameter values. In addition, it may indicate a term in position of a definition.
CAPITAL LETTERS	Names of keys and key sequences.
Minus sign ('-')	Indicates a combination of keys. For example, COMMAND-Q means to hold down the COMMAND key while pressing the Q key.
Exclamation mark	A warning about potential errors or any other important comment.

The following abbreviations are used in this manual:

- CPU – Central Processing Unit
- GUI – Graphical User Interface
- OS – Operating System
- RAM – Random Access Memory

Chapter 1. Introduction

Thank you for purchasing **Dr.Web Anti-virus for Mac OS X** (hereinafter referred to as **Dr.Web Anti-virus**). It offers reliable protection from various types of computer threats using the most advanced virus detection and neutralization technologies.

This manual is intended to help users of computers running Mac OS X install and use **Dr.Web Anti-virus**.

About Dr.Web Anti-virus

Dr.Web Anti-virus is an anti-virus solution designed to help users of computers running Mac OS X protect their machines from viruses and other types of threats.

The core components of the program (*anti-virus engine* and *virus databases*) are not only extremely effective and resource-sparing, but also cross-platform, which allows specialists in **Doctor Web** to create outstanding anti-virus solutions for different operating systems. Components of **Dr.Web Anti-virus** are constantly updated and virus databases are supplemented with new signatures to assure up-to-date protection. Also, a heuristic analyzer is used for additional protection against unknown viruses.

Main Components and Functions

Dr.Web Anti-virus consists of the following components each performing its own set of functions:

Component	Description
SpIDer Guard	This is a resident anti-virus component which checks all files (which are being used) in real time.
SpIDer Gate	This component checks the incoming HTTP traffic and blocks all malicious objets. It is also used to control access to web ressources.
Scanner	This virus-detection component is used for: • Express, full and custom system scan on user demand. • Neutralization of detected threats (Cure, Delete, Move to Quarantine). The action is either selected by the user manually, or automatically according to the **Dr.Web Anti-virus** settings for the corresponding type of threat.
Quarantine	This is a special folder which is used for isolation of infected files and other threats so that they cannot do harm to the system.
Updater	This is an automated updating utility that is used for updating virus databases and other program components.
License Manager	This component is used to simplify management of license key files, it allows to receive demo and license key files, view information about them and renew your license.

Flexible settings of **Dr.Web Anti-virus** allow to configure sound and on-screen notifications for various events, automatic actions applied by the anti-virus to detected threats, updates periodicity, list of files and folders excluded from scanning, etc.

Chapter 2. Installation and Removal

Dr.Web Anti-virus is distributed as a single disk image file (**drweb-1002-mac.dmg**). The file can be found on the product CD/DVD or downloaded via the Internet from the official **Doctor Web** website at http://www.drweb.com.

Dr.Web Anti-virus is not compatible with anti-virus software including its own earlier versions. Installing two anti-virus programs on one computer may lead to system crash and loss of important data. If you already have an anti-virus software installed, uninstall it before starting a new anti-virus installation.

System Requirements

Dr.Web Anti-virus can be installed on a computer running Mac OS X 10.7 or higher. Other requirements are similar to those of the operating system.

Installing and Removing Anti-virus

The **Dr.Web Anti-virus** software is distributed as a single disk image file (**drweb-1002-mac.dmg**).

To install Dr.Web Anti-virus

1. Double-click **drweb-1002-mac.dmg** to mount it, if necessary.
2. The License Agreement window will open. You need to read and accept it to continue the installation.
3. Drag the application file from the disk image to the **Applications** folder on your Mac.

To uninstall Dr.Web Anti-virus

To delete **Dr.Web Anti-virus**, you can simply move the application to **Trash**. If necessary, enter user name and password of the administrator account in the corresponding dialog.

Chapter 3. Managing Licenses

To use **Dr.Web Anti-virus** for an extended period of time, activate a license. You can purchase a license with the product or on the official **Doctor Web** website. A license allows to take advantage of all product features during the whole period. Parameters of the key file are set in accordance with the software license agreement. To register a new license, renew it after it is expired or get a new one, a special component - **License Manager** - is used.

It is recommended to register the license after installation because it unlocks updating, constant protection and on-demand scanning features.

If you want to evaluate the product before purchasing it, you can activate a demo period. It provides you with full functionality of the main components, but the period of validity is considerably restricted.

You can activate a demo period for the same computer no more than once a year.

Demo period is available for:

- 3 months. For that, register on the official **Doctor Web** website and receive a serial number.
- 1 month. For that purpose, no serial number is required and no registration data is requested.

License Key File

The license type is determined by a special file called the *key file*. The key file contains the following information:

- Duration of the anti-virus license
- List of components a user is allowed to use
- Other restrictions (for example, the number of users allowed to use the application)

A *valid* key for **Dr.Web Anti-virus** file satisfies the following criteria:

- License is not expired
- All anti-virus components required by the product are licensed
- Integrity of the key file is not violated

If any of the conditions is violated, the key file becomes *invalid* and **Dr.Web Anti-virus** stops detecting and neutralizing malicious programs in files, memory and email messages.

The key file has the .key extension and it can be received during the license registration procedure at first launch of **Dr.Web Anti-virus** via the License Manager.

The parameters of the key file which specify the user's rights are set in accordance with the License agreement. The file also contains information on the user and seller of the anti-virus.

It is recommended to keep the key file until the license or demo period expires.

A key file for a demo period activation can be used only on the computer where the registration procedure was run.

License Manager

To open **License Manager**, click **License Manager** in the application menu (the menu bar is at the top of the main desktop) or click the license information section in the main application window.

The **License Manager** window displays the information on your current license. The **Get New License** button allows you to register your license for **Dr.Web Anti-virus** or renew an expired license.

Registering License

After installation, you need to register **Dr.Web Anti-virus** to confirm legitimacy of using the anti-virus and unlock the updating, constant protection and on-demand scanning features.

When you run **Dr.Web Anti-virus** for the first time, registration starts automatically. You can also launch registration from License Manager by clicking **Get New License**.

To activate a new license

1. If you have a serial number for activation of a license or a demo period for 3 months, on the first step of the registration procedure, click **Activate license**.
2. Enter the serial number and click **Next**. In case you're activating a demo period, go to the step 5.
3. If you have a previous license, provide either its serial number or the corresponding key file. Select the corresponding option, then enter the serial number or drag the key file to the dotted area (alternatively, click the area to browse to select the key file).

   If you have been a user of **Dr.Web Anti-virus** in the past and are registering a new license, you are eligible for extension of your new license for another 150 days. If you are registering a renewal license and fail to provide a previous license key file, your new license period will be reduced by 150 days.

   Click **Next**.
4. Enter personal data (your given name, family name, and email address), select the country and enter the city name. All the fields listed are obligatory and should be filled in. If you want to receive news about **Doctor Web** by email, select the corresponding checkbox. Click **Next**.
5. The license key file will be downloaded and installed on your Mac. Usually, this procedure does not require your active participation. Click **Next**. If the activation procedure completed successfully, the corresponding message displays where the license validity period or demo period is specified. Click **Finish**. If activation failed, an error message displays.

To get demo

If you installed **Dr.Web Anti-virus** with demonstration purposes, select, click **Get demo**. You can activate a demo period to evaluate **Dr.Web Anti-virus**:

- For 3 months. For that, register on the website and receive a serial number.

  After you complete the questionnaire, a serial number required to activate the demo period for 3 months is sent to the specified email address.

- For 1 month. For that purpose, no serial number is required and no registration data is requested. The corresponding key file will be downloaded and installed automatically.

To purchase license

If you don't have a serial number, on the first step of the registration procedure, click **Purchase license** to purchase the license from **Doctor Web** online store.

It is recommended to keep the key file until it expires. If you re-install the product or install it on several computers, you will be able to use the previously registered license key file.

To install existing key file

1. On the first step of the registration procedure, click **Other activation types**.
2. If you already have a key file or a configuration file required to connect to the central protection server, drag it to the dotted area or click to browse to select the file.
3. To register you license, click **Next**. Usually, this procedure does not require your active participation.

Subsequent registration

You may need to reactivate a license or demo period if the key file is lost.

When reactivating a license or a demo period you receive the same key file as during the previous registration providing that the validity period is not expired.

A demo period can be reactivated only on the computer where the registration procedure was run.

The number of requests for a key file receipt is limited. One serial number can be registered not more than 25 times. If more requests are sent, the key file will not be delivered. In this case, to receive a lost key file, contact Technical Support describing your problem in detail, stating your personal data input during the registration and the serial number.

Chapter 4. Basic Functions

You can access all main functions from the **Dr.Web Anti-virus** window (see picture below). This window consists of sections that helps you control and access anti-virus components:

Section	Description
Desk	In this section, you can: • Enable or disable constant anti-virus protection. • Enable or disable web traffic check. • Review information about the last scan and start express or full system scan, as well as scan only critical files and folders. • Review information about the last virus databases update and start an update manually if necessary. • View information on the current license and run License Manager, if necessary. • Open the **Threats** or **My Dr.Web** section.
Threats	Lets you access the list of the detected threats, select actions to apply to them and to open the contents of Quarantine.
My Dr.Web	Lets you review the **Doctor Web** news, the latest special deals, the information on viruses and open your personal page on the official **Doctor Web** website, where you can review the information on your license, virus databases and last update, renew the license, contact Technical Support, etc.

Picture 1. Main application window.

Starting and Quitting Anti-virus

To start Dr.Web Anti-virus

Do one of the following:

- In the Finder, open the **Applications** folder and double-click **Dr.Web for Mac OS X**;
- Start the Launchpad and then select to start **Dr.Web for Mac OS X**.

On the application start the update settings are checked and the updates are downloaded, if necessary.

On the first start of the application the virus databases are updated to the most recent for the moment of application start. This may take some time.

To quit Dr.Web Anti-virus

Do one of the following:

- Click the **Quit Dr.Web for Mac OS X** item in the application menu (the menu bar is at the top of the main desktop).
- Click and hold the application icon in Dock, then select **Quit** in the menu.
- Press COMMAND-Q on the keyboard when **Dr.Web Anti-virus** is active.

When you quit **Dr.Web Anti-virus**, **SpIDer Guard** remains active. It is a resident anti-virus monitor which checks all files in real time when they are used.

Updating Anti-virus

Anti-virus solutions of **Doctor Web** use **Dr.Web** virus databases to detect malicious software. These databases contain details and signatures for all virus threats known at the moment of the product release. However, modern virus threats are characterized by high-speed evolvement and modification. Within several days and sometimes hours, new viruses and malicious programs emerge. To mitigate the risk of infection during the licensed period, **Doctor Web** provides you with regular updates to virus databases and product components, which are distributed via the Internet. With the updates, **Dr.Web Anti-virus** receives information required to detect new viruses, block their spreading and sometimes cure infected files which were incurable before. From time to time, the updates also include enhancements to anti-virus algorithms and fix bugs in software and documentation.

Updating the components and virus databases of **Dr.Web Anti-virus** ensures that your Mac's protection is always up to date and ready for any new threat types. Updating is performed by a special component called **Updater**.

On the first start of **Dr.Web Anti-virus** it is necessary to update the virus databases to the most recent for the moment of the application start. Further updates will be performed periodically, with interval specified in preferences of **Dr.Web Anti-virus**.

Configuring the update interval

1. In the application menu, click **Preferences** and open the **Update** tab.
2. Select an interval for updating.

Constant Anti-virus Protection

Constant anti-virus protection is carried out via a resident component called **SpIDer Guard**. The component performs real-time check of all files accessed by the user or running programs and processes running on your Mac. By default, it is enabled as soon as you install and register **Dr.Web Anti-virus**. Whenever a threat is detected, **SpIDer Guard** displays a warning and applies actions according to the anti-virus preferences.

To enable or disable SpIDer Guard

- On the **Desk** section of the main window (see Picture 1), enable/disable the **SpIDer Guard** option.
- Click the **Dr.Web Anti-virus** icon in the menu bar and select the corresponding item.

Only users with administrator privileges can disable **SpIDer Guard**.

Be extremely cautious when using this option! While **SpIDer Guard** functions are disabled, avoid connecting to the Internet and check all removable media using **Scanner** before accessing.

Scanning System On Demand

Dr.Web Anti-virus checks objects in the file system on your demand and detects various threats that may be present in the system though inactive. To protect your computer, it is necessary to run a system scan with **Dr.Web Anti-virus** periodically.

Process load increases during scanning which may lead to rapid discharge of batteries. We recommend starting scans when portable computers are powered by mains electricity.

To start system scanning

1. In the main window of **Dr.Web Anti-virus** select the scan mode:
   - **Express scan** – run a quick check of the most vulnerable parts of the system only.
   - **Full scan** – perform a full scan of the entire file system.

   You can press the hot keys combinations CONTROL-COMMAND-E and CONTROL-COMMAND-F on the keyboard to start express or full scan.

2. To scan only certain files and folders, drag them to the main application window or click the dotted area in the left part of the window to select objects to scan.

   In the list of objects select files and folders to scan:

   - To add an object to the list, click + under the list of objects or simply drag this object to the list.
   - To delete an object from the list, select it and click − or drag it outside the application window.

   Click **Start Scanning** to start scanning the selected objects.

To start a file or a folder scan from the context menu

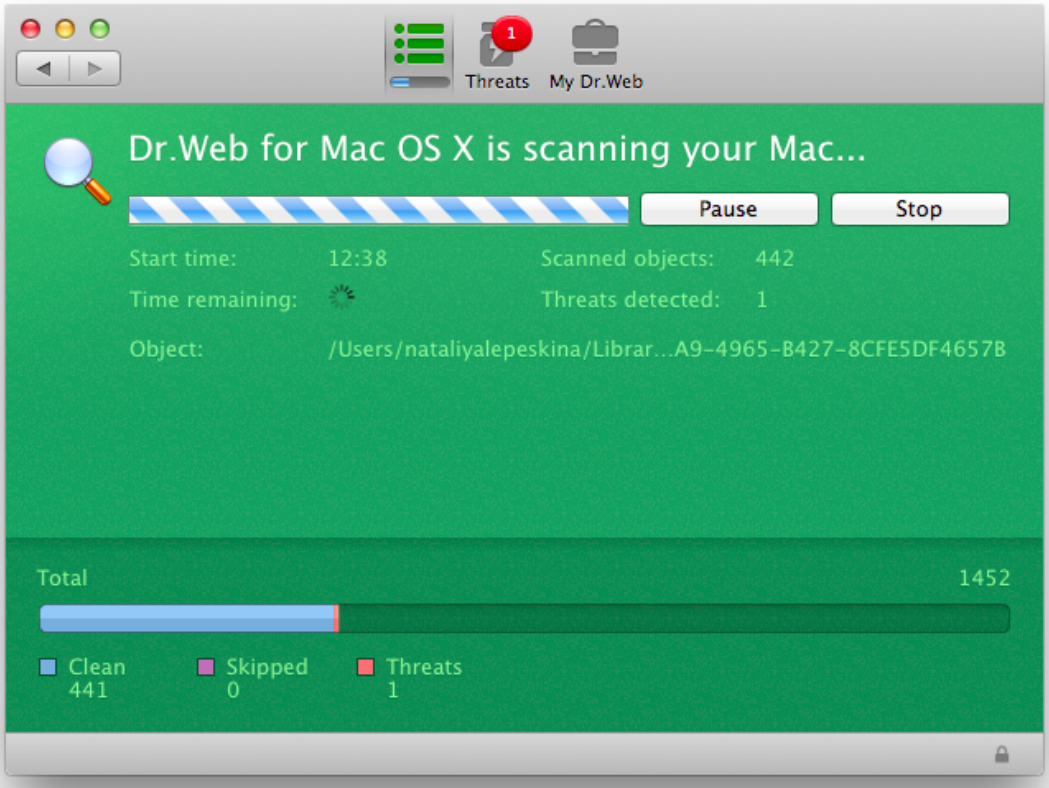
Select **Check with Dr.Web** in the context menu of the file or folder icon on the Desktop or in Finder.

When you start scanning, the main window switches to the results section (see the illustration below). During scanning, this section displays the following information:

- scanning start time
- number of checked objects
- time left to end scanning
- number of the detected threats
- name of the file that is currently being scanned

Statistic summary of the current scanning session is displayed in the bottom part of the window.

You can pause or stop scanning use the **Pause** and **Stop** buttons..



Picture 2. Viewing the scanning results.

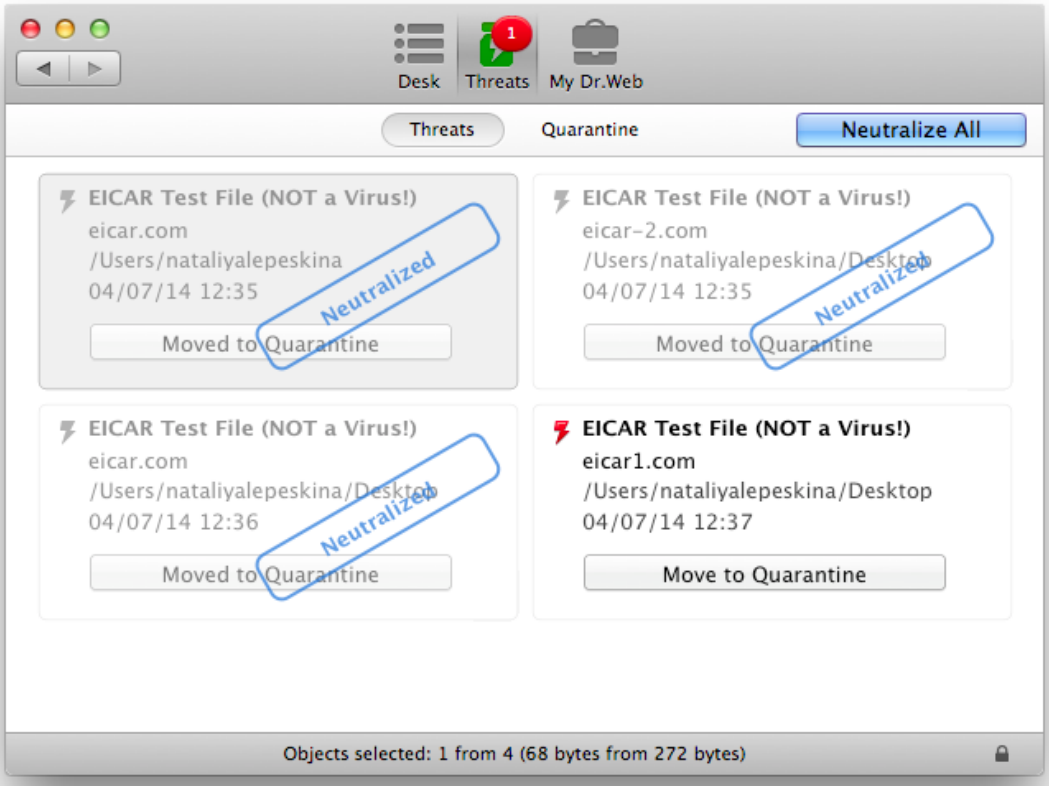
Some files may be omitted during scanning because they are corrupted or protected by password. If there are archives in the list of the skipped objects, try to extract them before scanning.

Dr.Web Anti-virus may require the administrator privileges to access and check critical areas of the hard drive. To grant **Dr.Web Anti-virus** administrator privileges:

- Press the combination COMMAND-SHIFT-A on the keyboard, then enter the administrator password.
- Click the lock icon in the bottom of the window and then enter the administrator password.

Neutralizing Threats

To neutralize threats, you can specify the automatic actions or apply actions to the threats manually. To review the list of detected threats and apply actions to neutralize them, open the **Threats** tab on the main application window (see illustration below).



Picture 3. Threats tab.

To view information on the threats

1. To view the list of the detected threats, open the **Threats** section. In the status bar in the bottom of the window the total number and size of the detected threats and also the number and size of the selected threats are displayed.
2. To view the information in a threat, click the button or double-click the threat.
3. To read about the type of the threat on **Doctor Web** website, click the button to the left of the threat name on the details window.

To neutralize the detected threats

1. Open the **Threats** section.
2. To apply an action specified in the anti-virus settings for the corresponding threat type, click the button with this action under the threat. To select an alternative action, click the arrow on the button with recommended action on the details window.
3. To neutralize several threats, select them (hold the SHIFT key to select multiple objects), then select the action to perform in the **Actions** section of the main application menu or in the context menu opened by right-clicking the list of the threats.

4. To neutralize all threats, click **Neutralize All**. This will apply actions specified in the anti-virus settings for the corresponding threat types.

You can also use the hot keys combinations on the keyboard to apply actions to the threats.

HTTP Traffic Check And Access Control to Web Resources

Web traffic check is carried out via a resident component called **SpIDer Gate**. It checks the incoming HTTP traffic and blocks all objects that contain security threats. HTTP is used by web browsers, download managers and other applications which exchange data with web servers, that is, which work with the Internet.

SpIDer Gate also allows you to control access to web resources and to prevent users from viewing undesirable websites (for example, pages on violence, gambling, adult content, etc.).

By default, **SpIDer Gate** is enabled automatically after you install and register **Dr.Web Anti-virus**.

Other applications for checking web traffic and controlling access to web resources installed on your Mac may not work properly if **SpIDer Gate** is enabled.

To enable or disable SpIDer Gate

- On the **Desk** section of the main window (see Picture 1), enable/disable the **SpIDer Gate** option.
- Click the **Dr.Web Anti-virus** icon in the menu bar and select the corresponding item.

Only users with administrator privileges can disable **SpIDer Gate**.

To configure HTTP traffic check

By default, **SpIDer Gate** blocks all incoming malicious objects. You can select the types of malicious programs to block, configure actions for the not checked objects and set up the maximum time for checking one file by performing the following actions:

1. In the application menu, click **Preferences** and open the **SpIDer Gate** tab. Only users with administrator privileges can change **SpIDer Gate** settings. Click the icon of a lock at the bottom of the window and enter the administrator name and password, if necessary.
2. Click **Advanced**.
3. Select the malware types to block.
4. Specify the maximum time for checking one file. Please note, that increasing the time for scanning a single may slow down your Mac in some cases.
5. By default, the objects that cannot be scanned are blocked. To allow such objects, clear the **Block not checked content** checkbox.
6. Click **OK** to save changes.

To configure access to websites

By default, in addition to HTTP traffic anti-virus check, **SpIDer Gate** blocks URLs listed due to a notice from copyright owner and not recommended sites. You can disable these functions on the **SpIDer Gate** tab of **Dr.Web Anti-virus** preferences. You can also select the website categories to block access to and create black and white lists of websites to automatically allow or block access to them regardless of other **SpIDer Gate** settings.

The default **SpIDer Gate** settings are optimal for most uses. Do not change them unnecessarily.

To configure the websites blocking parameters:

1. In the application menu, click **Preferences** and open the **SpIDer Gate** tab. Only users with administrator privileges can change **SpIDer Gate** settings. Click the icon of a lock at the bottom of the window and enter the administrator name and password, if necessary.
2. Select the categories of websites you want to block access to.
3. To create and manage the black and white lists of web addresses, click **Black And White Lists**. By default, both lists are empty. You can add addresses to the black and white lists. Click + under the corresponding list and enter a domain name or a part of a domain name for the website that you want block or allow access to:
   - To add a certain website, enter its name (for example, **www.example.com**). This allows access to all webpages located on this website.
   - To allow access to websites with similar names, enter the common part of their domain names. For example, if you enter example, then **SpIDer Gate** will allow access to the **example.com**, **example.test.com**, **test.com/example**, **test.example222.com** and other similar websites.
   - To allow access to websites within a particular domain, enter the domain name with a period ('**.**'). This allows access to all webpages located on this website. If the domain name includes a forward slash ('**/**'), the substring before the slash is considered a domain name, while the substring after the slash is considered a part of address for the websites that you want to access within this domain. For example, if you enter **example.com/test**, **SpIDer Gate** will allow access to webpages such as **example.com/test11**, **template.example.com/test22**, and so on.

   To delete websites from black or white list, select them in the corresponding list and click − or drag them outside the application window.
4. Click **OK** to save changes.

Getting Help

To get help about the program you can use **Dr.Web Help** which can be accessed via the Apple Help viewer.

To access Dr.Web Help

In the menu bar, click **Help** and select **Dr.Web Help**, or search for keywords using the text box.

If you cannot find a solution for your problem or necessary information about **Dr.Web Anti-virus**, you can request direct assistance from Technical Support.

Chapter 5. Advanced Use

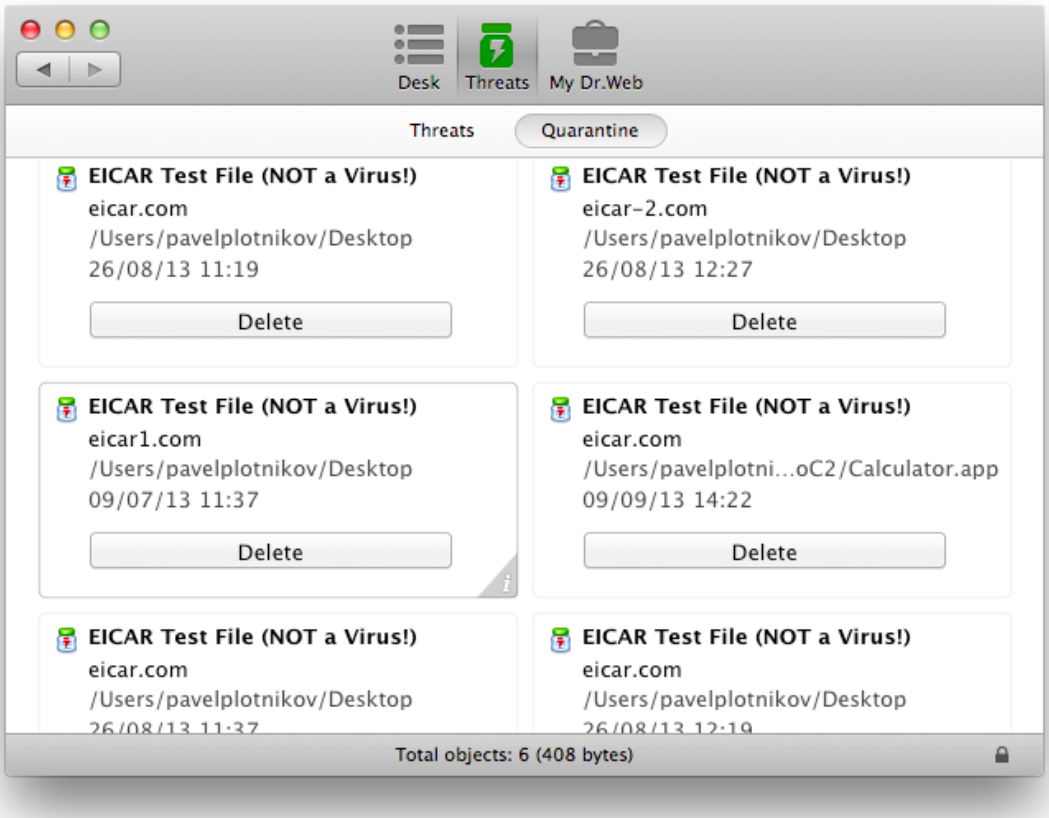
This chapter contains information on performing more advanced tasks with **Dr.Web Anti-virus** and adjusting its settings.

Quarantine

Quarantine allows you to isolate detected malicious or suspicious objects that cannot be cured from the rest of the system in case you need them. Curing algorithms are being constantly improved, therefore these objects may become curable after one of the updates.

Due to the privacy reasons, the quarantine folder is created for each user in the system. Therefore, if you switched to the administrator mode, the detected threats which are moved to the administrator **Quarantine** and will not be available in the user **Quarantine** folders.

You can view and manage the contents of quarantine using the **Quarantine** tab on the **Threats** section of the main window (see illustration below). In the status bar in the bottom of the window the total number and size of the threats and also the number and size of the selected threats are displayed.



Picture 4. Objects in quarantine.

To view information on the objects in quarantine

1. Click the button or double-click the object.
2. To read about the type of the threat that the object is supposed to contain on **Doctor Web** website, click the button to the left of the threat name on the details window. This will open the page with information on this type of threats on **Doctor Web** website.

To process objects in Quarantine

1. To apply a recommended action to an object in quarantine, click the button with this action under the object. To select an alternative action, click the arrow on the button with recommended action on the details window. You can select one of the following actions:
   - **Delete** – to completely remove the object from the file system.
   - **Cure** – for another attempt to cure the object.
   - **Restore** – to return the object from the quarantine to the initial folder it has been moved from.
   - **Restore to** – to select the folder to move the object from quarantine.
2. To process several objects, select them (hold the SHIFT key to select multiple objects), then select the action to perform in the **Actions** section of the main application menu or in the context menu opened by right-clicking the list of objects.

You can also use the hot keys combinations on the keyboard to apply actions to the objects in quarantine.

Configuring Automatic Actions

You can specify actions that will be applied automatically by **Dr.Web Anti-virus** to various types of computer threats unless it is required to choose an action manually. You can set different automatic reaction for **Scanner** and **SpIDer Guard**.

To configure automatic actions

1. To open the automatic reactions settings for **Dr.Web Anti-virus** components, do one of the following:
   - To configure automatic actions for **Scanner**, in the application menu, click **Preferences** and open the **Scanner** tab.
   - To configure automatic actions for **SpIDer Guard**, in the application menu, click **Preferences** and open the **SpIDer Guard** tab.
2. Select necessary action for infected, incurable nad suspicious objects.
3. Click **Other** to select actions for malware (adware, dialers, jokes, riskware and hacktools).
4. The actions specified in the **SpIDer Guard** settings will be applied automatically every time a threat is detected by this components. To apply action automatically to the threats detected during the system check performed by **Scanner**, select the **Apply actions automatically** checkbox in the **Scanner** settings section.
5. Click **Advanced** to set up the check of the complex objects (archives and email files) and specify the maximum time for scanning a single file. Please note, that scanning the contents of archives and email files, as well as increasing the time for scanning a single file leads to increasing of the overall scanning time and may slow down your Mac in some cases.

The default automatic actions are optimal for most uses. Do not change them unnecessarily.

By default, all **SpIDer Guard** settings are locked in order to prevent anyone without administrative privileges from changing these settings. To unlock them, select the **SpIDer Guard** section of the anti-virus preferences, click the icon of a lock at the bottom of the window and enter the administrator name and password.

Excluding Files from Scanning

You can make up a list of files and folders that should be excluded from scanning. You can set different exclusions for **Scanner** and **SpIDer Guard**.

To configure exclusions

1. In the application menu, click **Preferences** and open the **Exclusions** tab.
2. Select the **SpIDer Guard** and/or **Scanner** checkboxes next to the objects in the list of exclusions to exclude these objects from scanning.
3. If necessary, modify the list of exclusions:
   - To add a file or folder to the list, click the + button and select the object.
   - To delete object from the exclusions list, select it and click − or drag it outside the application window.

By default, all quarantine folders are excluded from scans of both components, because they are used to isolate detected threats and, as access to them is blocked, there is no use scanning these folders.

The default exclusions settings are optimal for most uses. Do not change them unnecessarily.

By default, all **SpIDer Guard** settings are locked in order to prevent anyone without administrative privileges from changing these settings. To unlock them, click the icon of a lock at the bottom of the window and enter the administrator name and password.

Notifications

The notifications about various events that may occur during operation of the anti-virus are configured on the **Main** tab of **Dr.Web Anti-virus** preferences.

There are 2 type of notifications:

- On-screen messages
- Sound alerts

By default, the notifications settings are locked in order to prevent anyone without administrator privileges from changing them. To unlock these settings, click the icon of a lock at the bottom of the preferences window and enter the administrator name and password.

To configure sound notifications

Sound alerts are enabled by default. To disable or enable sound alerts, clear or select the **Use sound alerts** checkbox on the **Main** tab of the application preferences.

To configure on-screen notifications

1. On-screen notifications are enabled by default. To disable or re-enable on-screen notifications, clear or select the **Enable notifications** checkbox on the **Main** tab of the application preferences.
2. Select the notification system:
   - **Dr.Web** (selected by default)
   - **System** (Mac OS X standard notifications)
   - **Growl**

3. For **Dr.Web** notifications, you can configure additional parameters by clicking **Configure** to the right of the selected notification system:
   - Specify the notifications display time
   - Select the area on the screen to show notifications

   Click **OK** to apply settings.

Administrator Privileges

Dr.Web Anti-virus may require administrator privileges to access and check critical areas of the hard drive. To start scanning with administrator privileges:

1. In the application menu click **Preferences** and open the **Main** tab.
2. Select the **Start scanning with administrator privileges** checkbox. You will need to enter the administrator password before scanning (express, full or custom) starts.

Optimizing Battery Use

By default, when your Mac is operating under battery power, the scanning is paused to prevent the battery from quick draining. **Dr.Web Anti-virus** displays a corresponding message where you can confirm pausing or continue scanning. To disable scanning pausing:

1. In the application menu click **Preferences** and open the **Main** tab.
2. If you don't want to pause scanning when you Mac is on battery power, clear the **Pause scanning when on battery power** checkbox.

Operation Mode

If necessary, you can use your installation of **Dr.Web Anti-virus** to connect to corporate anti-virus networks or to access **Dr.Web® AV-Desk** anti-virus service of your IT provider. To operate in such central protection mode, you do not need to install additional software or uninstall **Dr.Web Anti-virus**.

By default, **Dr.Web Anti-virus** mode settings are locked in order to prevent anyone without administrative privileges from changing these settings. To unlock them, click the icon of a lock at the bottom of the mode preferences window and enter the administrator name and password.

To use central protection mode

1. Contact an anti-virus network administrator of your company or IT provider for a public key file and parameters of connection to the central protection server.
2. In the application menu, click **Preferences** and select **Mode**.
3. To connect to central protection server of your company or IT provider, select the **Enable central protection mode** checkbox.

   In the central protection mode, the option of manual start and configuring updates is blocked. Some features and settings of **Dr.Web Anti-virus**, particularly concerning the constant protection and on-demand scanning, may be modified and blocked for compliance with the company security policy or according to the list of purchased services. A key file for operation in this mode is received from central protection server. Your personal key file is not used.

In central protection mode the scanning of your computer can be launched manually or according to schedule directly from the server.

4. On switching to the central protection mode **Dr.Web Anti-virus** restores parameters of the previous connection. If you are connecting to the server for the first time or connection parameters have changed, do the following:

The install.cfg file provided by administrator of anti-virus network contains settings to connect to the central protection server. To use this file:

1. Click **Other** activation types in the **License Manager**.
2. Drag the configuration file to the opened window or click the dotted area to select the file.

If the file is mounted, fields for entering the connection settings will be specified automatically.

- Enter the IP address of the central protection server provided by administrator of anti-virus network.
- Enter the port number that is used to connect to the server.
- Drag the public key file to the settings window, or double-click the public key area and browse to select the file.
- As an option, enter the authentification parameters: station ID, which is assigned to your computer for registration at the server, and password. The entered values are saved with Keychain system. Therefore, you need not enter them again when reconnecting to the server.

Depending of the authorization settings of the central protection server, the station can be connected to the server in one of the following modes:

- As a newbie. In this case it may require to be approved on the server (ID and password will be assigned automatically) or it may be authorized automatically if the corresponding authorization mode is specified on the server/
- If the station has already been created on the server and it has an ID and password, it will be authorized automatically when connecting to the server regardless of its settings.

For detailed information on connecting a station to the server refer to **Dr.Web Control Center** and **Dr.Web AV-Desk** Administrator guides.

To use standalone mode

1. In the application menu, click **Preferences** and select **Mode**.
2. To switch to the standalone mode, clear the **Enable central protection mode** checkbox.

   On switching to this mode, all settings of the anti-virus are unlocked and restored to their previous or default values. You can once again access all features of anti-virus.
3. For correct operation in standalone mode, **Dr.Web Anti-virus** requires a valid personal key file. The key files received from central protection server cannot be used in this mode. If necessary, you can receive or update a personal key file with License Manager.

Restoring Deafult Settings

If you experience any difficulties with configuring **Dr.Web Anti-virus**, you can restore the default application settings.

By default, the restoring defaults option is locked in order to prevent anyone without administrator privileges from changing it. To unlock it, click the icon of a lock at the bottom of the window and enter the administrator password.

1. In the application menu, click **Preferences** and open the **Main** tab.
2. Click **Restore Defaults**. Confirm restoring the default application configuration by clicking **Restore Now** in the corresponding dialog.

Appendices

Appendix A. Types of Computer Threats

Herein, the term *"threat"* is defined as any kind of software potentially or directly capable of inflicting damage to a computer or network and compromising the user's information or rights (that is, malicious and other unwanted software). In a wider sense, the term "threat" may be used to indicate any type of potential danger to the security of the computer or network (that is, vulnerabilities that can result in hacker attacks).

All of the program types stated below have the ability to endanger the user's data or confidentiality. Programs that do not conceal their presence (e.g. spam distribution software and various traffic analyzers) are usually not considered as computer threats, although they can become threats under certain circumstances.

In **Doctor Web** classification, all threats are divided according to the level of severity into two types:

- **Major threats** – classic computer threats that may perform destructive and illegal actions in the system on their own (erase or steal important data, crash networks, etc.). This type of computer threats consists of software that is traditionally referred to as malware (malicious software), that is, viruses, worms and Trojans.
- **Minor threats** – computer threats that are less dangerous than major threats, but may be used by a third person to perform malicious activity. Also, mere presence of minor threats in the system indicates its low protection level. Among IT security specialists this type of computer threats is sometimes referred to as grayware or PUP (potentially unwanted programs) and consists of the following program types: adware, dialers, jokes, riskware, hacktools.

Major threats

Computer Viruses

This type of computer threats is characterized by the ability to implement its code into other objects. Such implementation is called *infection*. In most cases, the infected file becomes a virus carrier itself and the implemented code does not necessarily match the original. Most viruses are intended to damage or destroy data in the system.

In **Doctor Web** classification, viruses are divided by the type of objects which they infect:

- **File viruses** infect files of the operating system (usually executable files and dynamic libraries) and activate upon launching of the infected file.
- **Macro-viruses** are viruses that infect documents used by Microsoft® Office and some other applications supporting macro commands (usually, written in Visual Basic). Macro commands are a type of implemented programs (macros) written in a fully functional programming language. For instance, in Microsoft® Word macros can automatically initiate upon opening (closing, saving, etc.) a document.
- **Script viruses** are created using script languages and usually infect other scripts (e.g. service files of an operating system). They are also able to infect other file formats that allow execution of scripts and thus take advantage of scripting vulnerabilities in Web applications.
- **Boot viruses** infect boot records of diskettes and partitions or master boot records of fixed disks. They require very little memory and remain ready to continue performing their tasks until a system roll-out, restart or shut-down occurs.

Most viruses have some kind of protection against detection. Protection methods are being constantly improved and ways to overcome them are constantly being developed. All viruses may also be classified according to the type of protection that they use:

- **Encrypted viruses** cipher their code upon every infection to hamper their detection in a file, boot sector or memory. All copies of such viruses contain only a small common code fragment (the decryption procedure) that can be used as a virus signature.
- **Polymorphic viruses** also encrypt there code, but besides that they also generate a special decryption procedure that is different in every copy of the virus. This means that such viruses do not have byte signatures.
- **Stealth viruses** perform certain actions to disguise their activity and thus conceal their presence in an infected object. Such viruses gather the characteristics of an object before infecting it and then plant these "dummy" characteristics that mislead the scanner searching for modified files.

Viruses can also be classified according to the programming language in which they are written (in most cases, it is Assembler, high-level programming languages, script languages, etc.) or according to affected operating systems.

Computer Worms

Worms have become a lot more widespread than viruses and other types of computer threats recently. Like viruses, they are able to reproduce themselves and spread their copies, but they do not infect other programs and files (that is, they do not need host files to spread). A worm infiltrates a computer from a worldwide or local network (usually via an attachment to an email) and distributes its functional copies to other computers in the network. It can begin distributing itself either upon a user's action or in an automatic mode choosing which computers to attack.

Worms do not necessarily consist of only one file (the worm's body). Many of them have an infectious part (the shellcode) that loads into the main memory (RAM) and then downloads the worm's body as an executable file via the network. If only the shellcode is present in the system, the worm can be deleted by simply restarting the system (at which the RAM is erased and reset). However, if the worm's body infiltrates the computer, then only an anti-virus program can cope with it.

Worms have the ability to cripple entire networks even if they do not bear any payload (i.e. do not cause any direct damage) due to their intensive distribution.

In **Doctor Web** classification, worms are divided by the method of distribution:

- **Net worms** distribute their copies via various network and file-sharing protocols.
- **Mail worms** spread themselves using email protocols (POP3, SMTP, etc.).
- **Chat worms** use protocols of popular messengers and chat programs (ICQ, IM, IRC, etc.).

Trojan Programs (Trojans)

This type of computer threats cannot reproduce itself or infect other programs. A Trojan substitutes a program that is used a lot and performs its functions (or imitates its operation). At the same time, it performs some malicious actions in the system (damages or deletes data, sends confidential information, etc.) or makes it possible for hacker to access the computer without permission, for example, to harm the computer of a third party.

A Trojan's masking and malicious facilities are similar to those of a virus. A Trojan may even be a component of a virus. However, most Trojans are distributed as separate executable files (through file-exchange servers, removable data carriers or email attachments) that are launched by users or system tasks.

It is very hard to classify Trojans due to the fact that they are often distributed by viruses or worms and also because many malicious actions that can be performed by other types of threats are ascribed to Trojans only. Here are some Trojan types which are distinguished as separate classes in **Doctor Web**:

- **Backdoors** are Trojans that make it possible for an intruder to log on into the system or obtain privileged functions bypassing any existing access and security measures. Backdoors do not infect files, but they write themselves into the registry modifying the registry keys.
- **Rootkits** are used to intercept system functions of an operating system in order to conceal themselves. Besides, a rootkit can conceal processes of other programs (e.g. other threats), registry keys, folders and files. It can be distributed either as an independent program or as a component of another malicious program. There are two kinds of rootkits according to the mode of operation: User Mode Rootkits (UMR) that operate in user mode (intercept functions of the user mode libraries) and Kernel Mode Rootkits (KMR) that operate in kernel mode (intercept functions on the level of the system kernel, which makes it harder to detect).
- **Keyloggers** are used to log data that users enter by means of a keyboard. The aim of this is to steal personal information (i.e. network passwords, logins, credit card data, etc.).
- **Clickers** redirect hyperlinks to certain addresses in order to increase traffic of websites or perform DDoS attacks.
- **Proxy Trojans** provide anonymous Internet access through a victim's computer.

Trojans may also perform other malicious actions besides those stated above, for example, change the start page in a Web browser or delete certain files. However, other actions can also be performed by other types of threats (viruses and worms).

Minor Threats

Hacktools

Hacktools are programs designed to assist the intruder with hacking. The most common among them are port scanners that detect vulnerabilities in firewalls and other components of computer protection system. Besides hackers, such tools are used by administrators to check security of their networks. Occasionally, common software that can be used for hacking and various programs that use social engineering techniques are designated as among hacktools as well.

Adware

Usually, this term refers to a program code implemented into freeware programs that force display of advertisements to users. However, sometimes such codes can be distributed via other malicious programs and show advertisements in Web browsers. Many adware programs operate with data collected by spyware.

Jokes

Like adware, this type of minor threats can not be used to inflict any direct damage to the system. Joke programs usually just generate messages about errors that never occurred and threaten to perform actions that will lead to data loss. Their purpose is to frighten or annoy users.

Dialers

These are special programs that are designed to scan a range of telephone numbers and find those where a modem answers. These numbers are then used to mark up the price of telephoning facilities or to connect the user to expensive telephone services.

Riskware

These programs were not intended as computer threats, but can potentially cripple or be used to cripple system security due to certain features and, therefore, are classified as minor threats. Riskware programs are not only those that can accidentally damage or delete data, but also ones that can be used by crackers or some malicious programs to do harm to the system. Among such programs are various remote chat and administrative tools, FTP-servers, etc.

Suspicious Objects

These are possible computer threats detected by the heuristic analyzer. Such objects can potentially be any type of threat (even unknown to IT security specialists) or turn out safe in case of a false detection.

Suspicious objects should be sent for analysis to the **Dr.Web Virus Laboratory**.

Appendix B. Fighting Computer Threats

The **Dr.Web** anti-virus solutions use several malicious software detection methods simultaneously, and that allows them to perform thorough checks on suspicious files and control software behavior.

Detection Methods

Signature analysis

The scans begin with signature analysis which is performed by comparison of file code segments to the known virus signatures. A *signature* is a finite continuous sequence of bytes which is necessary and sufficient to identify a specific virus. To reduce the size of the signature dictionary, the **Dr.Web** anti-virus solutions use signature checksums instead of complete signature sequences. Checksums uniquely identify signatures, which preserves correctness of virus detection and neutralization. The **Dr.Web virus databases** are composed so that some entries can be used to detect not just specific viruses, but whole classes of threats.

Origins Tracing

On completion of signature analysis, the **Dr.Web** anti-virus solutions use the unique **Origins Tracing™** method to detect new and modified viruses which use the known infection mechanisms. Thus, **Dr.Web** users are protected against such threats as notorious blackmailer Trojan.Encoder.18 (also known as gpcode). In addition to detection of new and modified viruses, the **Origins Tracing™** mechanism allows to considerably reduce the number of false triggering of the heuristics analyzer. Objects detected using the **Origins Tracing™** algorithm are indicated with the `.Origin` extension added to their names.

Execution emulation

The technology of program code emulation is used for detection of polymorphic and encrypted viruses, when the search against checksums cannot be applied directly, or is very difficult to be performed (due to the impossibility of building secure signatures). The method implies simulating the execution of an analyzed code by an *emulator* – a programming model of the processor and runtime environment. The emulator operates with protected memory area (*emulation buffer*), in which execution of the analyzed program is modelled instruction by instruction. However, none of these instructions is actually executed by the CPU. When the emulator receives a file infected with a polymorphic virus, the result of the emulation is a decrypted virus body, which is then easily determined by searching against signature checksums.

Heuristic analysis

The detection method used by the heuristics analyzer is based on certain knowledge (*heuristics*) about certain features (attributes) than might be typical for the virus code itself, and vice versa, that are extremely rare in viruses. Each attribute has a weight coefficient which determines the level of its severity and reliability. The weight coefficient can be positive if the corresponding attribute is indicative of a malicious code or negative if the attribute is uncharacteristic of a computer threat. Depending on the sum weight of a file, the heuristics analyzer calculates the probability of unknown virus infection. If the threshold is exceeded, the heuristic analyzer generates the conclusion that the analyzed object is probably infected with an unknown virus.

The heuristics analyzer also uses the **FLY-CODE™** technology, which is a versatile algorithm for extracting files. The technology allows making heuristic assumptions about the presence of malicious objects in files compressed not only by packagers **Dr.Web** is aware of, but by also new, previously unexplored programs. While checking packed objects, **Dr.Web** anti-virus solutions also use structural entropy analysis. The technology detects threats by arranging pieces of code; thus, one database entry allows identification of a substantial portion of threats packed with the same polymorphous packager.

As any system of hypothesis testing under uncertainty, the heuristics analyzer may commit type I or

type II errors (omit viruses or raise false alarms). Thus, objects detected by the heuristics analyzer are treated as "suspicious".

While performing any of the abovementioned checks, the **Dr.Web** anti-virus solutions use the most recent information about known malicious software. As soon as experts of **Doctor Web Virus Laboratory** discover new threats, the update for virus signatures, behavior characteristics and attributes is issued. In some cases updates can be issued several times per hour. Therefore even if a brand new virus passes through the **Dr.Web** resident guards and penetrates the system, then after an update the virus is detected in the list of processes and neutralized.

Actions

To neutralize computer threats, **Dr.Web products** use a number of actions that can be applied to malicious objects. A user can leave the default settings, configure which actions to apply automatically, or choose actions manually upon every detection. Below is a list of possible actions:

- **Cure** is an action that can only be applied to major threats (viruses, worms and Trojans). It implies deletion of malicious code from infected objects as well as recovery of their structure and operability to the state in which it was before the infection if possible. Sometimes malicious objects are made of malicious code only (for example, Trojans or functional copies of computer worms) and for such objects to cure the system means to remove the whole object completely. Not all files infected by viruses can be cured, but curing algorithms evolve all the time.
- **Quarantine** (Move to Quarantine) is an action when the detected threat is moved to a special folder and isolated from the rest of the system. This action is preferable in cases when curing is impossible and for all suspicious objects. It is recommended to send copies of such files to the **Dr.Web Virus Laboratory** for analysis.
- **Delete** is the most effective action for neutralizing computer threats. It can be applied to any type of computer threat. Note that deletion will sometimes be applied to certain objects for which the Cure action was selected. This will happen in cases if the object consists of only malicious code and have no useful information (for example, curing a computer worm implies deletion of all its functional copies).
- **Rename** is an action when the extension of an infected file is changed according to a specified mask (by default, the fist character of the extension is replaced with #). This action may be appropriate for files of other operating systems (such as MS-DOS® or Microsoft® Windows®) detected heuristically as suspicious. Renaming helps to avoid accidental startup of executable files in these operating systems and therefore prevents infection by a possible virus and its further expansion.
- **Ignore** is an action applicable to minor treats only (that is, adware, dialers, jokes, hacktools and riskware) that instructs to skip the threat without performing any action or displaying information in report.
- **Report** means that no action is applied to the object and the treat is only listed in results report.

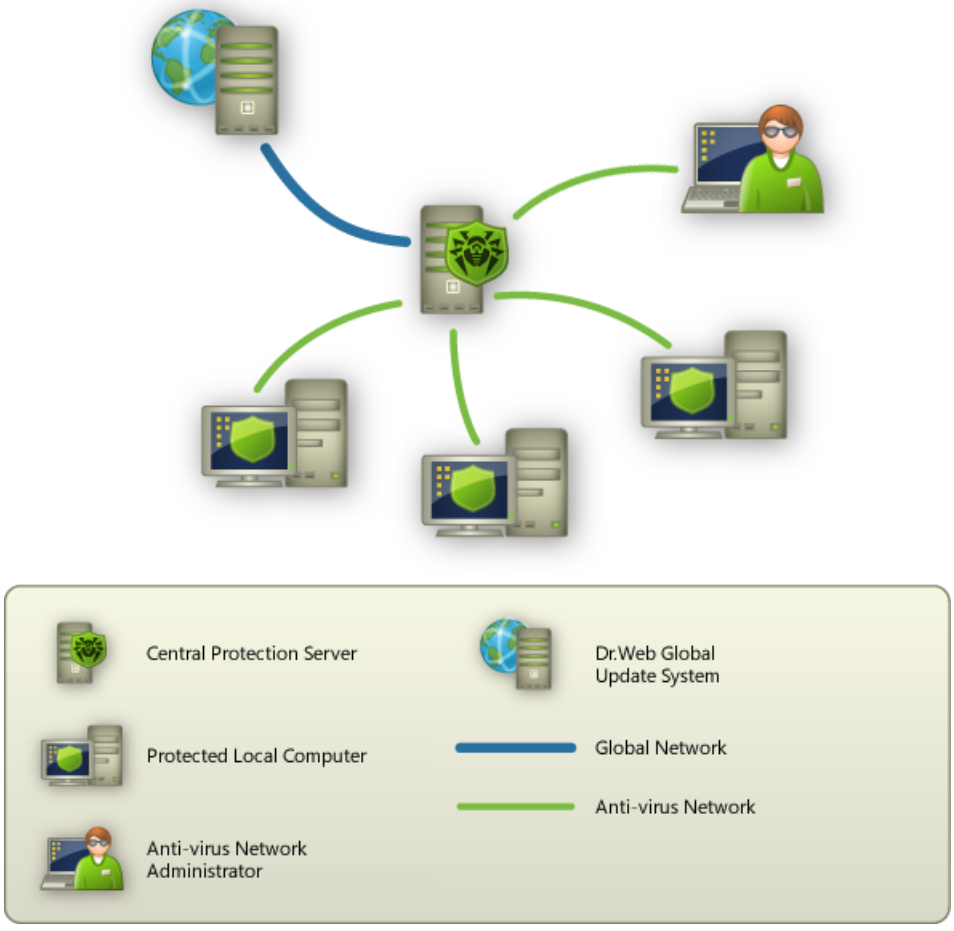
Appendix C. Central Anti-virus Protection

Solutions for central protection from **Doctor Web** help automate and simplify configuring and managing information security of computers within logical structures (for example, company computers that access each other from both inside and outside of company's local networks). Protected computers are united in one anti-virus network which security is monitored and managed from central server by administrators. Connection to centralized anti-virus systems guarantees high level of protection while requiring minimum efforts from end-users.

Logical Structure of Anti-virus Networks

Solutions for central protection from **Doctor Web** use client-server model (see picture below).

Workstations and servers are protected by *local anti-virus components* (agents, or clients; herein, **Dr.Web Anti-virus**) installed on them, which provides for anti-virus protection of remote computers and ensures easy connection to central protection server.



Picture 5. Logical structure of anti-virus networks.

Local computers are updated and configured from *central server*. The stream of instructions, data and statistics in the anti-virus network goes also through the central protection server. The volume of traffic between protected computers and the central server can be quite sizeable, therefore solutions provide options for traffic compression. To prevent leak of sensitive data or substitution of software downloaded onto protected computers, encryption is also supported.

All necessary updates are downloaded to central protection server from **Dr.Web Global Update System** servers.

Local anti-virus components are configured and managed from central protection server according to commands from *anti-virus network administrators*. Administrators manage central protection servers and topology of anti-virus networks (for example, validate connections to central protection server from remote computers) and configure operation of local anti-virus components when necessary.

Local anti-virus components are not compatible with other anti-virus software including versions of **Dr.Web anti-virus solutions** that do not support operation in central protection mode (i.e. **Dr.Web Anti-virus for Mac OS X** version 5.0). Installing two anti-virus programs on one computer may lead to system crash and loss of important data.

Central Protection Solutions

Dr.Web® Enterprise Security Suite

Dr.Web® Enterprise Security Suite is a complex solution for corporate networks of any size that provides reliable protection of workstations, mail and file servers from all types of modern computer threats. This solution also provides diverse tools for anti-virus network administrators that allow them to keep track and manage operation of local anti-virus components including components deployment and update, network status monitoring, statistics gathering, and notification on virus events.

Dr.Web® AV-Desk Internet Service

Dr.Web® AV-Desk is an innovative Internet service created by **Doctor Web** for providers of various types of Internet services. With this solution, providers can deliver information security services to home customers and companies providing them with a selected package of services for protection from viruses, spam and other types of computer threats for as long as is necessary. Services are provided online.

For more information on **Dr.Web® AV-Desk** Internet service, visit the official **Doctor Web** website at http://www.av-desk.com.

Appendix D. Hot Keys

You can use the special hot keys combinations to start a system scan, to apply action to the detected threats or to set up **Dr.Web Anti-virus**.

Combination		Description
Scan menu	CONTROL-COMMAND-E	Express scan
	CONTROL-COMMAND-F	Full scan
	CONTROL-COMMAND-C	Select objects to scan
Actions menu	COMMAND-SHIFT-C	Cure
	COMMAND-SHIFT-M	Move to Quarantine
	COMMAND-SHIFT-I	Ignore
	COMMAND-SHIFT-D	Delete
	COMMAND-SHIFT-R	Restore
	COMMAND-SHIFT-P	Restore to
	COMMAND-SHIFT-A	Work with administrator privileges
General	COMMAND-,	Preferences
	COMMAND-A	Select all
	COMMAND-W	Close

Appendix E. Contacting Support

If you encounter any issues installing or using company products, take advantage of the following **Doctor Web** support options:

- Download and review the latest manuals and guides at http://download.drweb.com/
- Read the frequently asked questions at http://support.drweb.com/
- Browse **Dr.Web** official forum at http://forum.drweb.com/

If you have not found solution for the problem, you can request direct assistance from **Doctor Web Technical Support** by filling in the web-from in the corresponding section of the support site at http://support.drweb.com/.

For regional office information, visit the **official Doctor Web website** at http://company.drweb.com/contacts/moscow.

Index

Index